Aug 10th, 12:00 AM

Why are some Internet users more prone to adopt prudent Cybersecurity practices than others?

Ashish A. Kakar
Texas Tech University, ashish.kakar@ttu.edu

Bismita Choudhury
Assam Down Town University, bismita.choudhury@adtu.in

Akshay Kakar
University of Houston, akakar@uh.edu

Why are some Internet users more prone to adopt prudent Cybersecurity practices than others?

Completed Research

Ashish Kakar
Texas Tech University
ashish.kakar@ttu.edu

Bismita Chowdhury
Assam down town University
bismi.choudhury@gmail.com

Akshay Kakar
University of Houston
akakar@uh.edu

Abstract

In this first of its kind study, we use the regulatory focus theory to suggest that some types of internet users are more vulnerable to cybersecurity threats than others. A questionnaire based survey was conducted with 222 students of a large public university. The findings of the study show that users with preventive focus were more likely to adopt and implement cybersecurity best practices than those with promotion focus. They also reported lesser number of cybersecurity attacks than students with promotion focus. The findings of the study are not only useful to the student community but also to organizations that employ them currently or will do so in future. Future avenues for research are also suggested for identifying and securing vulnerable internet users.

Keywords

Preventive focus, promotion focus, cybersecurity attitude.

Introduction

More than four billion people, constituting over half world's population is online (https://wearesocial.com/us/blog/2018/01/global-digital-report-2018). Users are also increasingly putting out their information online. However, the internet is not a secured space (Hall, 2012) . Further, there are not many regulations that protect the users. It is therefore not surprising that the internet has become a hacker's paradise. Although cybersecurity technologies have become increasingly sophisticated, so have the hackers. Additionally, the weakest link in cybersecurity as in other security technologies is considered to be the human element (Pfleeger and Caputo, 2012). Attitudes such as operating system patches and security software updates are annoying, time-consuming and can be ignored; that it is acceptable to downloaded free movies and unauthorized software; and that security settings can be turned off are not uncommon (Chandarman and Van Niekerk, 2017).

Hackers understand this and exploit human vulnerabilities to the hilt to commit cybercrimes. To compound the problem, most users do not even know the various ways their information can be exposed to hackers with malicious intent (West, 2008; Ramalingam et al., 2016). They are also often unaware that their information is compromised until after the damage is done. Many have heard of the havoc caused by cybersecurity breaches but have a false sense of security that bad things happen to other people (Johnston and Warkentin, 2010). Users are often smug and confident in their belief that their information and identities are well protected until disaster strikes.

Yet, for those who are interested, there is a lot of information and sites which provide good information and advice on how to secure the information on your devices as well as cyber space such as the site (https://staysafeonline.org) run by the National Cyber Security Alliance (NCSA) and the US-Cyber Emergency Response Team (US-CERT) tips for end users (http://www.us-cert.gov/cas/tips/). There are

also awareness programs conducted by organizations that can help users secure information from hackers. However, we know from experience that few users pay heed to such advice or are scrupulous about adopting good cybersecurity practices.

The question is whether we can identify such individuals? Conversely, do we know which type of individuals are lax about adopting cyber security practices? Lax attitudes about cybersecurity not only puts the individual but also the organization and other individuals at risk. Identifying such individuals will help organizations focus their attention on such high-risk individuals to keep information more secure.

To find answers to the aforementioned questions, we suggest that the regulatory focus of individuals, a personality trait, can help identify the individuals who are serious about cyber security and those who are not. To test our theory, we conduct a study with university students of a R1 research university. Students are the largest single user group of Internet (China Internet Network Information Center, 2018) and often considered a more vulnerable group. A compulsive need to remain connected exposes them to increased online risks (Aliyu, Abdallah, Lasisi, Diyar and Zeki, 2010l; Mochiko, 2016). Research has shown that 55% of students aged 18-29 years experienced some form of data theft (Olmstead and Smith (2017). Additionally, many students are in the forefront of knowledge creation and generate as well as use a lot of information while at the university. Further, the same students are/ will be the current/ future employees of organizations. Thus, they form a high impact group for investigation of cybersecurity issues and for getting answers to the questions posed in the study.

Literature Review

Cyber Security Threats

Cyberattacks are increasing in both sophistication and quantity with over 65% of users becoming victim to some form of cybercrime (Symantec, 2013; LaBrie et al., 2010). The weakest link in cybersecurity is considered to be the human element which is exploited by cyber criminals to commit a wide range of cybercrimes (Chandarman and Van Niekerk, 2017; Clark et al. 2011). Technology by itself has failed to protect users and organizations from cyberthreats (Anwar et al., 2016; Herath and Rao, 2009a b). The advancements in technologies that protect against cybercrime is often negated by human error putting their organizations and themselves at risk (Hadlington, 2017). Research has shown that 50% of the worst security breaches are due to inadvertent human error (PWC, 2015).
In this study we therefore investigate attitudes and behaviors that make users vulnerable to the most common types of cyberattacks listed in literature:

1. Phishing
2. Malware
3. Social Engineering
4. Password usage
5. Downloads from unreliable sources

Phishing is considered to be the biggest cybersecurity threat and cybercrimes due to phishing are increasing year after year (https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf). Typically, in phishing hackers send emails to a large number of people at random in the hope that some of them will be tricked into providing sensitive information. When emails are sent to specific targets with a view to commit cybercrime it is called spear phishing. In spear phishing hackers research information about individuals or companies before launching devastating cyberattacks. Some high-profile victims of spearfishing include organizations such as RSA and Google, USA State department and the White House, the Democratic Nation Committee and John Podesta, chair of Hillary Clinton's 2016 U.S. presidential campaign (Ho, Sharma, Javed, Paxson and Wagner, 2017).

Malware is a malicious software written with the intention of gaining access to or causing harm to devices, data or people. There are various types of malware such as computer viruses, spyware, trojans, ransomware and worms. Malware is becoming increasingly sophisticated and is capable of causing great harm to both people and organizations who become its victim (https://purplesec.us/resources/cyber-security-statistics/).

Social engineering is becoming a major cybersecurity risk in virtual communities (Krombholz, Hobel, Huber and Weippl, 2015). Unlike malware which attacks computer systems, social engineering is an art of psychologically manipulating users to gain access to critical information. Also, unlike malware technical protection is often ineffective against social engineering attacks. Phishing is often used interchangeably with social engineering. While both social engineering and spear fishing target a small number of users after researching information about them, social engineering involves using many other psychological methods such as pre-texting, quid pro quo and tail gating and use devices in addition to email attachments and webpages such as the phone or online chats to entice their victims.

Hackers also often use music, copied textbooks and movies as digital baits to entice unsuspecting users to download them. These downloaded files have embedded malware which can infect your computer system and gain access to sensitive personal or financial information. The malware can then spread from your computer system to other computer systems connected on the network putting other users in your network at risk.

Passwords are the users' Achilles heel in the Internet full of sophisticated hackers The National Cyber Security Centre (NCSC) in the United Kingdom found that 23.2 million victim accounts worldwide used "123456" as their passwords (NCSC, 2019). Research has found that users still use the weak passwords as they did thirty years earlier despite sustained user education(Stewart and Martin, 1994; Morris and Thompson, 1979; Herly, 2009). Thus, awareness programs by themselves may not be the answer to changing human cybersecurity attitudes and behavior.

Regulatory Focus Theory

In their search for enduring human factors that contribute to risky cyber behavior, researchers have examined the role of personality. For example, Uebelacker and Quiel, (2014) examined the effect of the key personality factors such as the Big Five Personality traits and individuals' susceptibility to social engineering; Egelman and Peer (2015b) and Coutlee et al. (2014) investigated the effect on individuals' impulsiveness and on cyber risk-taking behavior; McBride et al. (2012) examined the effect of personality traits such as extraversion and introversion on security policy violations and Shropshire, Warkentin, Johnston, and Schmidt (2006) and Shropshire et al. (2015) examined the impact of agreeableness and conscientiousness on individuals' compliance with security protocols. These studies have advanced our understanding of individual differences in cyber behavior and attitude and how they impact cyber security.

In this study we investigate the role of regulatory focus (RF) an enduring personality trait and its effect on individual's behavior and attitude towards cyber security. Keeping in view, the success of RF theory in identifying risk taking behavior in a wide variety of contexts, we feel this tested theory would be ideal for identifying which individuals are likely to flout security norms and prudent practices and which individuals are more likely to conform to them.

The theory of regulatory focus postulates two different self-regulatory systems to achieve a goal. People can either target their attention towards the achievement of ideals and gains, or towards the fulfillment of duties and the avoidance of losses (Werth and Forester 2005a). Depending on how individuals direct their attention, they find themselves in either a so-called promotion or prevention focus (Higgins 1997). People with promotion focus have a high concern for the absence or presence positive outcomes while people with prevention focus have a high concern for the absence or presence negative outcomes (Wirtz and Lwin, 2009).

Thus, the user response to actual or potential gains and losses will vary for people with prevention and promotion focus. People with prevention focus are likely to behave in a safe and responsible manner. They are very attentive and careful about avoiding undesired states (they are anxious not to make mistakes) (Werth and Forster 2007). By contrast, people with promotion focus aspire for achievement of ideals and accomplishments. These tenets of the regulatory focus theory has been applied successfully and found to be valid in areas ranging from entrepreneurship, organizational citizenship behaviors, employee work outcomes, alliance development, strategic decision making, consumers' product choice and mergers and acquisitions (e.g., Chernev 2004; Chitturi, Raghunathan and Mahajan 2007; Brockner, Higgins and Low, 2004; Dewett and Denisi, 2007; Crowe and Higgins, 1997; Gamache, McNamara, Mannor and Johnson, 2015; Das and Kumar, 2011). We use the regulatory focus theory in this article to understand how the user

adoption of prudent cyber security practices will vary among users of promotion and prevention focus to address security threats.

Based on themes gleaned through a review of literature we identified a few high impact attitudes and behaviors that can either put users at risk or help in reducing their cyber security vulnerability. By limiting the attitude-behavior pairs in our study (see Appendix A) we hoped to user response on cyber security attitudes and behavior. Limiting the questions would mitigate participant fatigue which can prevent thoughtful responses from participants. The goal is to accurately identify individual differences in cyber attitudes and behavior and how their impact varies with people of promotion and prevention focus in thwarting/ promoting cybersecurity attacks

Hypothesis Development

People with prevention focus fear failures and take necessary steps to avoid undesirable outcomes (Crowe and Higgins, 1997). They are not only skeptical of information presented to them but also cautious in sharing information (Molden et al., 2008). Trust is primarily a promotion response and concern a typically preventive response (Downing and Hoy, 2000). The vigilant attitude of people with prevention focus makes them less trustful of strangers than people with promotion focus (Hosmer, 1995). They are therefore less likely to fall victim to social engineering. Further, privacy concern is a largely defensive response (Sheehan and Hoy, 2000) more likely to be exhibited by people with prevention focus. They are therefore less likely to have weak passwords, skimp on security settings and updates, and fall victim to social engineering and phishing.

Losses loom larger than gains for these individuals. They are less likely to take risks even though the returns maybe high such as using pirated software or downloading free movies and textbooks. Therefore, taking necessary security precautions to avoid unpleasant outcomes will be a priority for them. Furthermore, individuals with a prevention focus are more inclined to initiate actions earlier than their promotion-focused counterparts do (Freitas, Liberman, Salovey, & Higgins, 2002) such as ensuring timely security updates, thereby reducing security vulnerabilities. They will diligently spend time and energy on prudent practices such as having a secure password, implement appropriate security settings in a timely manner and investing in malware protection software.

By contrast, those in a promotion focus have a "risky" response bias, compared with compared to the "conservative" response bias of those in prevention focus (Crowe and Higgins, 1997). People with promotion focus are concerned with reducing errors of omission. Gains loom larger in their calculus than losses. They are therefore likely to be more adventurous in pursuit of advancement and gains. Promotion focused individuals are scared of losing opportunities and are likely to be more trustful of strangers (Hosmer, 1995). In pursuit of their goals they are likely to take more risks than people with prevention focus. One can therefore expect them to be less heedful of security and safety issues Users with promotion focus will thus have a greater chance of falling victim to social engineering, have weak passwords, use pirated software and download free music, movies and textbooks than those with prevention focus, thereby likely to become a prime target for cyberattacks and leading us to the following hypotheses.

Hypothesis 1: Users with prevention focus are more likely to demonstrate prudent cybersecurity attitudes than users with promotion focus

Hypothesis 2: Users with promotion focus are less likely to demonstrate prudent cybersecurity behaviors than users with prevention focus

People with prevention focus are concerned with reducing errors of commission and are likely to behave in a cautious and precautionary manner (Crowe and Higgins, 1997). They are more sensitive to loss-related information (Molden et al., 2008) and are in a state of vigilance to assure safety (see Brendl & Higgins, 1995; Higgins, 1996a; Higgins et al., 1994). They will therefore take efforts to learn about cybersecurity good practices and stay updated with new developments. The prudent cybersecurity attitudes and behaviors of users with preventive focus will likely reduce their vulnerability to security attacks.

Hypothesis 3: Users with prevention focus will be less vulnerable to cyberattacks than users with promotion focus

Method

Study Setting and Design

This study was conducted in a university setting with student subjects. Each subject in the study answered a questionnaire-based survey that captured data on demographics and the users' response to the attitude and behavior questions listed in Appendix A. To determine the chronic regulatory focus of individuals the questions from the 11 item scale developed by Higgins, Tory, Friedman, Harlow, Idson, Ayduk and Taylor (2001) were used. The sample size for the study was determined based on the effect size found during a preliminary study. The preliminary study was used to pilot the full-scale study by pre-testing the survey instrument. The study was conducted with 64 subjects. Assuming a power of 0.8, alpha=0.05 (one tail) and taking in consideration the large effect size obtained in the preliminary study, a look up of Cohen's power primer (Cohen, 1992) gave the sample size of 54 subjects.

Subjects

The subjects for the study were recruited from a R1 public university in the United States. The college of business of this university encourages research exposure by awarding extra credit to students for research participation. An email was sent to all 2304 students of the college of business at the beginning of the semester inviting them to participate in the study. Only those students who agreed to provide data on security attacks/ incidents were recruited for the study. We received a total of 240 responses. Based on this response we invited all 240 students to participate in the study. Among those invited to participate only 222 actually provided the data in of the survey. The subjects were 19-23 years old. 51.3% respondents were female, and 49.7% respondents were male.

Measures Used

The subject behavior and attitude responses were taken based on a questionnaire from Appendix A and the 11 item (RFQ) Regulatory Focus Questionnaire (Higgins, Tory, Friedman, Harlow, Idson, Ayduk and Taylor, 2001) consisting of two subscales assessing chronic prevention and promotion focus was used to ascertain individuals' dispositional or chronic regulatory focus.

All the above measures used a 9-point Likert scale with anchors of 1 (strongly disagree) and 9 (strongly agree). Scale items were averaged to create an overall value for each construct. Responses were coded such that high levels of the constructs are represented by high values for cybersecurity attitudes and behaviors. The high values for items assessing regulatory focus represented promotion focus and low values represented prevention focus. The purpose of the study was only revealed during the debriefing session. The items in the questionnaire were scrambled to prevent hypothesis guessing. Some items were reverse coded.

Procedure

Subjects answered the questionnaire-based survey and also reported on the details of security attacks, if any, which they faced in the last 3 months. The period was kept short by design to help participants recall the incidents easily. To mitigate demand and social desirability bis, the participants were informed at the beginning of the study that their responses will be kept confidential even from the researchers and would be identified with unique questionnaire numbers only to represent student response.

Method of Analyses

To establish reliability and validity of the measures used in the study factor analysis was performed on the data set. Subjects were classified into chronic prevention or chronic promotion focused categories based on the median split on the difference between their RFQ promotion and RFQ prevention scores in the sample (e.g., Louro, Pieters and Zeelenberg, 2005; Avnet and Higgins, 2006). Users with Promotion focus were coded as 1 and users with Prevention focus were coded as 0. Two sample t-tests were performed for across user group comparison of behavior and attitude towards cybersecurity. A difference in proportion test was used to compare the security attacks on users with prevention focus versus users with promotion focus.

Results and Analysis

Factor analysis procedure was done using IBM SPSS Statistics Version 19. R1 to R11 represented items in the regulatory focus scale including promotion and prevention subscales). Convergent and discriminant validity between scales were evident by the high loadings within factors, and no significant (> .40) cross loadings among factors. Significant differences were found in cybersecurity attitudes and behavior in prevention vs promotion groups (see Tables 1 and 2). Except in their attitude towards password, users with preventive focus reported a more positive attitude and behavior towards cybersecurity than users with promotion focus.

	Survey Item Description	**Prevention Focus**		**Promotion Focus**		**Difference in Mean**
		Mean	**SD**	**Mean**	**SD**	
1	My friends would not send me anything malicious or scams through email	6.32	0.37	4.53	0.47	1.79**
2	Installing and Updating security software is too time consuming and annoying	6.03	0.73	5.21	0.46	0.82*
3	The security settings and tools slow me down and are pesky. I turn them off or disable them.	6.54	0.65	4.62	1.02	1.92**
4	It is a waste of time to change passwords because you can still get hacked	7.36	0.18	6.15	0.64	1.21*
5	It is too difficult and cumbersome to remember difficult passwords	6.51	0.80	6.09	0.46	.42
6	Strong passwords do not help much. If a hacker wants to access your account he will be able to do it anyway	6.78	0.79	5.11	0.44	1.67**
7	It is worth the risk downloading an important file or useful software it is worth downloading it from the Internet	6.72	0.86	5.71	0.93	1.01*
8	I am generally inclined to read all my emails as anyone of them might turn out to be important for me - there is not much security risk as the email server will filter out suspicious/ unauthorized emails if any.	7.23	1.17	6.14	1.02	1.09*

*** p < .05 ** p < .01 ***p<.001**

Table 1. Differences in User Cybersecurity Attitudes in Prevention vs Promotion groups

	Survey Item Description	Prevention Focus		Promotion Focus		Difference in Mean
		Mean	SD	Mean	SD	
1	I share my passwords with my friends and/or relatives and/ or strangers	6.21	0.59	4.63	0.44	1.58**
2	I have installed Malware protection software on all my computer and devices and check at least once a week if they are updated R	5.91	0.62	5.14	0.67	0.77*
3	I choose security settings carefully on all my computers and devices R	6.34	0.43	4.75	0.82	1.59**
4	I never use the same username and password on each of my accounts and change each of them periodically on all my accounts R	7.45	0.34	6.01	0.65	1.44**
5	I use passwords that are easy for me to remember	6.78	0.67	5.23	0.39	1.55**
6	I generally use strong complex passwords that are more than 8 characters and consist of lowercase, uppercase, numbers, special characters R	7.32	0.72	4.68	0.48	2.64***
7	I refrain from downloading files and software from an untrusted or unknown source R	6.54	0.55	5.23	0.55	1.31**
8	I always check to see if the email address of the sender is suspicious and never click on hyperlinks in the email R	7.77	0.39	5.51	0.7	2.26***

*** p < .05 ** p < .01 ***p<.001**

Table 2. Differences in User Cybersecurity Behavior in Prevention vs Promotion groups

The total number of security incidents reported by students in the previous 3 months was 39 of which 12 were reported by 113 students who were categorized as preventive focused and 27 were reported by 109 students who were categorized as promotion focused. A difference in proportion test showed that the difference was significant (p<=0.05) – students with promotion focus were more likely to be victims of cyberattacks that students with prevention focus.

Discussion and Contribution

In this study on cybersecurity we focused on human factors rather than technology. Overall, all three hypotheses were supported. The study thus makes a unique contribution to literature by identifying internet users who are more prone to cyberattacks. As predicted the attitudes and behaviors of users were found to vary based on regulatory focus of the users. Users with prevention focus displayed better attitudes and behaviors and as a result faced significantly fewer security incidents than those with promotion focus.

The findings have practical implications. Students are heavy users of internet and technology managers of the future. Based on study findings, organizations having a high need of privacy and security can now identify and employ people with appropriate cyber attitudes and behavior to reduce security incidents. They can also identify based on the regulatory focus which individuals are more risk prone and take appropriate actions to influence their attitudes and behavior. Their security managers and analysts could

preferably be people who in addition to their technical skills are prevention focused. as one can expect them to be more cautious, vigilant and alert to cyber security risks. Organizations can also tailor their cybersecurity awareness programs depending on the chronic regulatory focus of users.

However, the study is not without its limitations. The results of the study cannot be generalized beyond the student population. Future studies may validate the findings of the study for other user groups such as the employees of organizations or older users of Internet such as retirees. Further, longitudinal studies should be conducted to determine whether regulatory focus is an enduring personality factor as has been assumed in the study or whether it varies with time. Additionally, whether the cybersecurity attitudes and behavior also vary with time or remain more or less static. A longitudinal study might also provide interesting insights into the relationship between the variables used in the study.

Another limitation of the study is that self-report measures were used in the study. Using self-report measures assumes that users possess accurate insights into their own experiences and motivations. Nonetheless, this concern is alleviated to the extent that regulatory focus scale used in the study has been tested across multiple studies and have been shown to have the requisite predictive validity. Also, the hypothesis for the effect of regulatory focus was tested for multiple dependent variables such as attitude, behavior and actual security incidents and found to be supported thereby generating confidence in the findings.

REFERENCE

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010, December). Computer security and ethics awareness among IIUM students: An empirical study. In *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010* (pp. A52-A56). IEEE.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Brendl, C. M., Higgins, E. T., & Lemm, K. M. (1995). Sensitivity to varying gains and losses: The role of self-discrepancies and event framing. *Journal of personality and social psychology*, *69*(6), 1028.

Brockner, J., Higgins, E. T., & Low, M. B. (2004). Regulatory focus theory and the entrepreneurial process. *Journal of business venturing*, *19*(2), 203-220.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, *20*, 133-155.

China Internet Network Information Center. (2018) The 41st China Statistical Report on Internet Development. [Available from: https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf]

Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K., & Blaze, M. (2011, August). Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In *USENIX Security Symposium* (Vol. 2011, pp. 8-12).

Cohen, J. (1992). "A power primer," *Psychological Bulletin* (112), pp. 155–159.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. A. (2014). An Abbreviated Impulsiveness Scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. *Archives of scientific psychology*, *2*(1), 1.

Crowe, E., & Higgins, E. T. (1997). Regulatory focus and strategic inclinations: Promotion and prevention in decision-making. *Organizational behavior and human decision processes*, *69*(2), 117-132.

Das, T. K., & Kumar, R. (2011). Regulatory focus and opportunism in the alliance development process. *Journal of Management*, *37*(3), 682-708.

Dewett, T., & Denisi, A. S. (2007). What motivates organizational citizenship behaviours? Exploring the role of regulatory focus theory. *European Journal of Work and Organizational Psychology*, *16*(3), 241-260.

Egelman, S., & Peer, E. (2015, September). The myth of the average user: Improving privacy and security systems through individualization. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 16-28).

Freitas, A. L., Liberman, N., Salovey, P., & Higgins, E. T. (2002). When to begin? Regulatory focus and initiating goal pursuit. *Personality and Social Psychology Bulletin*, *28*(1), 121-130.

Gamache, D. L., McNamara, G., Mannor, M. J., & Johnson, R. E. (2015). Motivated to acquire? The impact of CEO regulatory focus on firm acquisitions. *Academy of Management Journal*, *58*(4), 1261-1282.

Grove, A.S., 1996. Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career. Doubleday, New York. Grove, A. S. (1996). *Only the paranoid survive: How to exploit the crisis points that challenge every company and career*. Broadway Business.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

Hall, C. (2012). Security of the Internet and the Known Unknowns. *Communications of the ACM*, *55*(6), 35-37.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144).

Higgins, E. T. (1996). The" self digest": self-knowledge serving self-regulatory functions. *Journal of personality and social psychology*, *71*(6), 1062.

Higgins, E. T., Roney, C. J., Crowe, E., & Hymes, C. (1994). Ideal versus ought predilections for approach and avoidance distinct self-regulatory systems. *Journal of personality and social psychology*, *66*(2), 276.

Ho, G., Sharma, A., Javed, M., Paxson, V., & Wagner, D. (2017). Detecting credential spearphishing in enterprise settings. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 469-485).

Hosmer, Larue T. (1995), "Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics," *Academy of Management Rev*iew, 20 (2), 379 – 403.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

LaBrie, J., Collier, A., Palmer, A., 2010. Cybercrime Report: The Human Impact.

Lisa Vaas. How hackers broke into John Podesta, DNC Gmail accounts. https: //nakedsecurity.sophos.com/2016/ 10/25/how-hackers-broke-into- john-podesta-dnc-gmail-accounts/, October 2016.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, *5*(1), 1.

Merritt, M. (2010). *Norton" s Cybercrime Report: The Human Impact*. Retrieved 1/03/2012, 2012, from http://community. norton. com/t5/Ask-Marian/Norton-s-Cybercrime-Report-The-Human-Impact-Reveals-Global/ba-p/282432.

Mochiko, T. (2016, November 22). Cybercrime "will rise" with internet of things. *Business Live*. Retrieved from https://www.businesslive.co.za/bd/life/gadgets-and-gear/2016-11- 22-cybercrime-will-rise-with-internet-of-things

Molden, D. C., Lee, A. Y., & Higgins, E. T. (2008). Motivations for promotion and prevention. *Handbook of motivation science*, 169-187.

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, *22*(11), 594-597.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, *26*, 311-327. China Internet Network Information Center (2016). *Research Report on Internet Surfing Behavior among Chinese Adolescent*. Available at: http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/qsnbg/201608/P020160812393489128332.pdf

Peter Bright. Spearphishing + zero-day: RSA hack not "extremely sophisticated". http://arstechnica.com/security/ 2011/04/spearphishing-0-day-rsa- hack-not-extremely-sophisticated/, April 2011.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

PWC. 2015 Information Security Breaches Survey. https://www.gov.uk/government

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. *arXiv preprint arXiv:1602.06510*.
Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.
Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security*, *49*, 177-191.
Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, 415.
Spear phishing: The top ten worst cyber-attacks. https://blog.cloudmark.com/wp-content/uploads/2016/01/cloud mark_ top_ten_infographic.png.
Stewart, D. W., & Martin, I. M. (1994). Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy & Marketing*, *13*(1), 1-19.
Symantec. (2013). *2013 Norton report: Cost per cybercrime victim up 50 percent*. Retrieved from http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01
Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.
West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34.
Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research*, *12*(2), 190-2.

APPENDIX A

A	My friends would not send me anything malicious or scams through email
B	**I share my passwords with my friends and/or relatives and/ or strangers**
A	Installing and Updating security software is too time consuming and annoying
B	**I have installed Malware protection software on all my computer and devices and check at least once a week if they are updated R**
A	The security settings and tools slow me down and are pesky. I turn them off or disable them.
B	**I choose security settings carefully on all my computers and devices R**
A	It is a waste of time to change passwords because you can still get hacked
B	**I never use the same username and password on each of my accounts and change each of them periodically on all my accounts R**
A	It is too difficult and cumbersome to remember difficult passwords
B	**I use passwords that are easy for me to remember**
A	Strong passwords do not help much. If a hacker wants to access your account he will be able to do it anyway
B	**I generally use strong complex passwords that are more than 8 characters and consist of lowercase, uppercase, numbers, special characters R**
A	It is worth the risk downloading an important file or useful software it is worth downloading it from the Internet
B	**I refrain from downloading files and software from an untrusted or unknown source R**
A	I am generally inclined to read all my emails as anyone of them might turn out to be important for me - there is not much security risk as the email server will filter out suspicious/ unauthorized emails if any.
B	**I always check to see if the email address of the sender is suspicious and never click on hyperlinks in the email R**

A=Attitude question, B=Behavior question, R=reverse coded questions